M.Sc. (IT) 4th Semester Examination 2024

Information System Security

MSIT0028E

Full Marks: 70 **Time: 3 hours**

The figure in the margin indicate full marks for the question

Answer Question **No 1**(**compulsory**) and **Any Five** from the rest

1. **Answer All questions**
   a. What do you mean by Firewall?
   b. What do you mean by Meet-in-the-Middle attack?
   c. Define Confusion and Diffusion.
   d. Discuss IP Spoofing vs IP Sniffing.
   e. How does a freeware different from malware?

5X2=10

2.
   a. Explain Symmetric and Asymmetric key cryptosystem with example. Also differentiate them.
   b. What all services are provided by network security? Discuss them.

(3+3) +6 =12

3.
   a. Explain Diffie-Hellman algorithm with example.
   b. How an intruder can get access while exchanging the key? Explain.

6+6=12

4.
   a. What is PGP? Discuss PGP authentication and confidentiality with diagram.
   b. What is message digest? How it plays the role in security.

(2+6) +4 =12

5.
   a. Find public and private keys for two given prime numbers p = 17 and q =11 using RSA algorithm. (Show each steps)
   b. Explain different types of attacks (at least two each from passive and active attack).

6+6 =12

6.
   a. Among Stream & Block cipher, which one is preferred and why?
   b. Explain two algorithms from each (Stream & Block cipher) with necessary diagrams.

2+10=12

7.
   a. What is S/MIME and how does it work?
   b. Explain Privacy Enhanced Mail (PEM) and it's working principle.

6+6 =12

8.
   With neat diagram, discuss the Block cipher modes of operation with merits and demerits.

12

9.
   a. Explain Feistel structure. How does DES works? Explain.
   b. Discuss different methods of public key distribution.

4+8 =12